

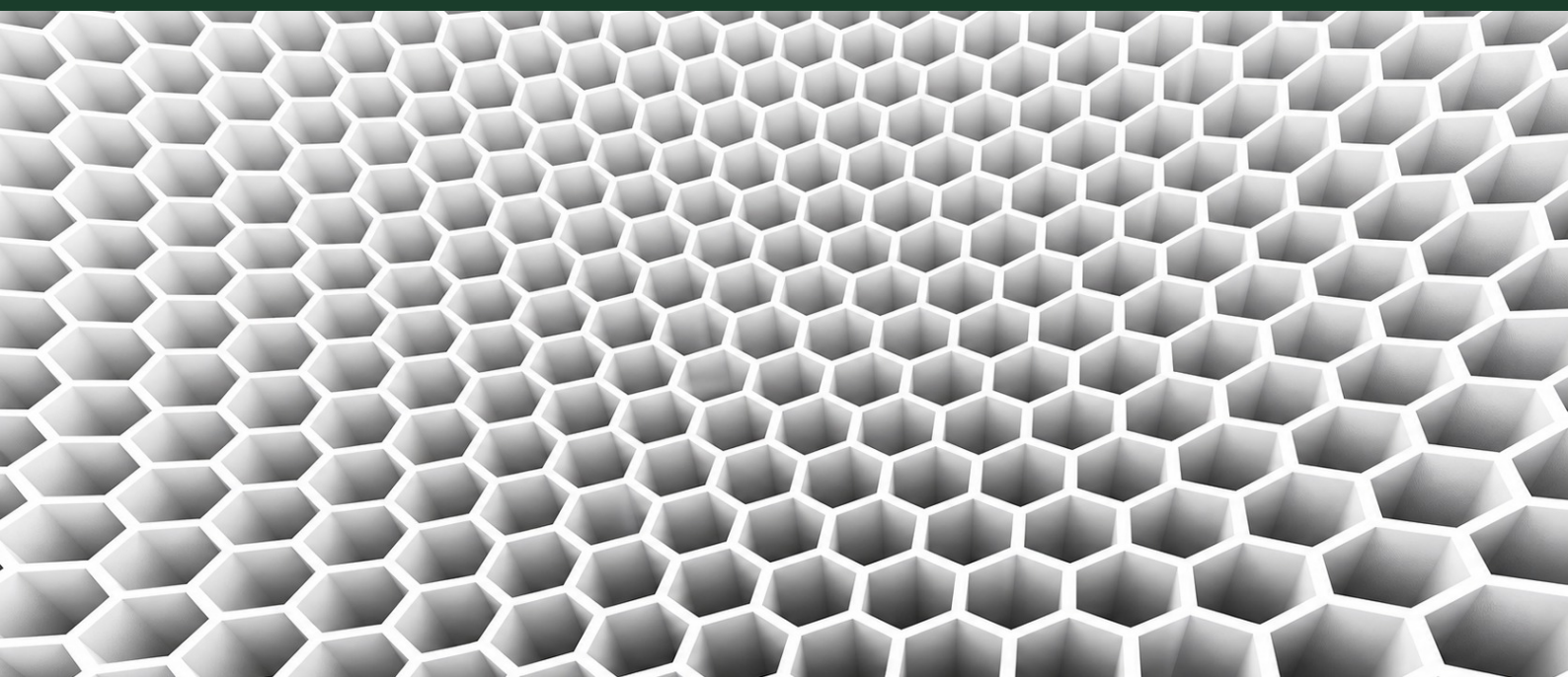
BEYOND SECURITY PROJECTS

Cybersecurity Is Not a Technology Project: Remote Work Turned It into a Permanent Change Programme

A 2021 operating case for governing identity, resilience, suppliers and security outcomes together

Giovanni Leonardi

December 2021



Contents

1. Executive Summary	3
2. The Threat Landscape Changed Shape	4
3. What Organisations Tried	4
3.1 Control deployment programmes	5
3.2 Compliance remediation	5
3.3 Awareness campaigns	5
3.4 Incident-driven mobilisation	5
4. Why Security Projects Produce Insecure Operations	6
4.1 Technical completion arrives before operational ownership	6
4.2 Security requirements compete with service outcomes	6
4.3 Measures describe activity rather than exposure	6
5. The Strong Case Against a Permanent Programme	7
6. Five Outcomes for Security Transformation	7
7. A Better Programme Architecture	8
7.1 Start with critical services	8
7.2 Build risk-based waves	8
7.3 Integrate security with change portfolios	8
7.4 Fund control operation, not only control purchase	9
7.5 Govern exceptions as a portfolio	9
8. Decision Rights and Roles	9
9. Evidence That Matters	10
10. A Twelve-Month Transition	11
11. Recommendation	11

Cybersecurity Is Not a Technology Project: Remote Work Turned It into a Permanent Change Programme

Programme · No. 242

Originally written December 2021 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

"Volume is not risk reduction."

1. Executive Summary

The security perimeter did not disappear when work moved away from offices in 2020. It multiplied. By the end of 2021, organisations are protecting identities used from homes and shared spaces, devices that rarely touch a corporate network, rapidly adopted cloud services, new supplier connections and operational processes redesigned under emergency pressure.

Many responses have treated this as a technology problem: buy stronger controls, close remote-access gaps, scan more frequently and train employees again. Those actions are necessary, but they fail when they are not connected to operating change. A control deployed without process ownership becomes an exception factory. A policy tightened without understanding the work creates bypasses. A vulnerability programme that counts patches but cannot change a legacy service produces reassuring activity while exposure accumulates.

Cybersecurity must now be governed as a programme of continuing organisational change. This does not mean creating a permanent project office around the security function. It means managing security outcomes across technology, operations, people, suppliers, data and investment through explicit decision rights, sequenced change and operational evidence.

A representative 2021 transformation illustrates the pattern. After remote access expanded from 1,800 to 14,500 users, an organisation launched seventeen security initiatives. Twelve delivered their technical milestones, yet privileged accounts remained unresolved, supplier connections were poorly inventoried and recovery tests exposed dependencies nobody owned. Progress appeared strong because projects reported installation rather than changed exposure.

This paper recommends a security transformation programme built around five outcomes: trustworthy identity, controlled devices and services, resilient critical operations, governed suppliers and prepared response. The model uses risk-based waves, accountable business owners, architecture and service integration, adoption measures, attack-informed testing and a quarterly decision cycle. Its purpose is not to promise perfect protection. It is to make risk reduction visible, prioritised and sustainable as work

continues to change.

2. The Threat Landscape Changed Shape

The early remote-work response was an extraordinary act of operational improvisation. Access capacity was expanded, equipment was issued, collaboration services were adopted and controls were varied so essential work could continue. Decisions that would ordinarily take months were made in days.

The security consequence was not one new vulnerability. It was a change in the organisation's topology.

Before 2020, many controls assumed that employees, devices and applications were concentrated behind managed network boundaries. That assumption was already weakening through cloud adoption, outsourcing, mobile working and digital supply chains. The pandemic accelerated the change and removed the remaining comfort of gradual transition.

By late 2021, the recurring exposure pattern includes:

- Identity becoming the primary route into services
- Personal and lightly managed environments surrounding corporate devices
- Remote administration expanding for employees and suppliers
- Data moving through rapidly adopted collaboration and cloud services
- Legacy applications exposed through new access routes
- Informal workarounds becoming persistent operating practices
- Supplier and software dependencies carrying risk across organisational boundaries
- Ransomware turning recovery capability into a board-level question

Attackers benefit from the joins: an old account, a weak supplier connection, a delayed patch on an internet-facing service, a convincing message during operational disruption or a privileged credential used without sufficient control. These are rarely owned by one security tool or one function.

The threat landscape after remote work is therefore best understood as a system of changed dependencies, not as a larger collection of technical threats.

Remote work did not simply move users outside the perimeter; it exposed how many security decisions had never belonged to the perimeter in the first place.

3. What Organisations Tried

The first wave of security action was understandably tactical. Capacity and continuity came first. During 2021, organisations have attempted to turn those emergency controls into a stronger posture. Four approaches recur.

3.1 Control deployment programmes

These initiatives implement multi-factor authentication, endpoint protection, improved logging, vulnerability scanning, email controls, data safeguards or network segmentation. They offer clear scope, technical ownership and measurable installation.

They work when the control maps to a defined population, process and service consequence. They fail when “deployed” is treated as equivalent to “effective”.

A composite organisation reported multi-factor authentication at 96 per cent. Investigation showed that the remaining four per cent included 63 service accounts and 18 privileged administrative routes supporting critical systems. The coverage measure celebrated volume while concealing consequence.

3.2 Compliance remediation

Audit findings, regulatory requirements and policy gaps are converted into plans with owners and deadlines. This creates senior attention and an evidential trail.

It works when findings are translated into operating outcomes. It fails when closure means a document, a configuration snapshot or a one-time sample. Security conditions change faster than annual evidence cycles.

One access-review project closed after every business unit submitted a signed return. Three months later, a sample of 500 accounts found 47 with inappropriate access because role changes had not been integrated into the joiner, mover and leaver process. The review had proved that managers could complete a campaign. It had not repaired the control mechanism.

3.3 Awareness campaigns

Employees receive training, simulated phishing exercises and regular communications. These actions recognise that human judgement matters.

They work when they are connected to specific workflows and easy reporting. They fail when users are treated as the weak link while systems continue to place impossible decisions in front of them.

An employee presented with an urgent supplier bank-change request, an unfamiliar remote login prompt and a project deadline is not failing simply because a training completion score is low. The process has combined authority, urgency and ambiguity without an independent verification route.

3.4 Incident-driven mobilisation

After a serious event, resources are concentrated, executives engage and remediation accelerates. This can resolve long-standing blockers.

It works because consequence is visible and authority is available. It fails when the organisation disbands the mobilisation after immediate containment, leaving root causes fragmented across unfunded teams.

The shared weakness is not lack of effort. It is that each approach treats a portion of the security outcome as a bounded intervention. The organisation installs, attests, trains or remediates, then returns ownership to an operating model that may not be able to sustain the change.

4. Why Security Projects Produce Insecure Operations

A project succeeds by delivering agreed scope within constraints. Security succeeds when exposure remains within appetite while threats, services and behaviour change. Those are different completion conditions.

Three mechanisms explain the gap.

4.1 Technical completion arrives before operational ownership

A new control is configured, but nobody funds the exception queue, tunes alerts, handles failed enrolments or decides which legacy services must be retired. The project hands over a capability; operations inherits a workload.

In the composite transformation, endpoint protection was installed on 12,800 devices. The project achieved 98 per cent deployment. Within eight weeks, the security operations team had 1,900 unresolved alerts and 740 devices had not reported for more than fourteen days. The installation milestone was true. The protection outcome was not.

4.2 Security requirements compete with service outcomes

Business teams experience controls as delay, friction or reduced flexibility. When security cannot express the consequence of a requirement, the service owner sees only cost. Exceptions multiply, often approved one at a time without understanding cumulative exposure.

The solution is not for security to own the business decision. It is to make the trade-off explicit: which service outcome is protected, what control is proposed, what operational burden it creates, what residual risk remains and who may accept it.

4.3 Measures describe activity rather than exposure

Boards receive patch counts, training completion, alerts, findings and maturity scores. These measures can improve while critical risks remain unchanged.

A useful measure must connect action to a security outcome. “Ninety-five per cent of vulnerabilities closed” is weaker than “all internet-facing critical vulnerabilities remediated within the agreed time, with three exceptions approved and compensating controls verified.”

Volume is not risk reduction.

5. The Strong Case Against a Permanent Programme

There is a serious objection to describing cybersecurity as a programme. Security is a continuing operational responsibility. Programmes are temporary. Creating another transformation layer can distance accountability from technology and service teams, add reporting overhead and encourage the belief that security will eventually be “finished”.

That objection is correct if the proposal is a permanent central project office.

The answer is a programme of outcomes with temporary waves of change, not a never-ending project. The enduring operating model owns controls and risk. The programme exists to change that operating model across boundaries that no single service team can resolve.

A security programme should close a wave when:

- The control mechanism operates in business-as-usual teams
- Exceptions have accountable owners and expiry
- Measures show changed exposure
- Recovery or response has been tested
- Funding and capacity are embedded
- Residual risk has been accepted at the right level

The programme then redirects attention to the next material change in the landscape. It does not retain work merely to preserve itself.

6. Five Outcomes for Security Transformation

A coherent programme needs outcomes broad enough to cross projects but specific enough to govern decisions.

Outcome	Core question	Evidence of change
Trustworthy identity	Can every material access be tied to a verified person or controlled service identity?	Privileged and high-risk access verified, monitored and reviewed
Controlled devices and services	Do connected assets meet minimum control conditions throughout use?	Coverage, health, exceptions and retirement visible by criticality
Resilient critical operations	Can essential services continue or recover after compromise?	Tested recovery, dependency evidence and known recovery limits
Governed suppliers	Are external access, software and data dependencies understood and controlled?	Critical suppliers mapped, access constrained and assurance tied to service risk

Outcome	Core question	Evidence of change
Prepared response	Can the organisation detect, decide and act at the speed of a serious incident?	Exercises, decision rights, communications and remediation proven

These outcomes are interdependent. Identity controls cannot compensate for an untested recovery route. Supplier assurance cannot protect a service whose assets are unknown. Awareness cannot repair an approval process that invites impersonation.

The programme board should govern the relationships among outcomes rather than sponsor a list of unrelated security projects.

7. A Better Programme Architecture

7.1 Start with critical services

Do not begin with every asset or every control. Identify the services whose loss, corruption or misuse would cause material operational, customer, safety, financial or regulatory harm.

For each service, map:

- Business owner and accountable technology owner
- Users, privileged roles and service identities
- Devices, applications, data and key interfaces
- External suppliers and remote connections
- Required recovery time and recovery dependencies
- Known control exceptions
- Current change activity

This creates an outcome-centred view. It also exposes where the same identity platform, supplier or legacy component creates concentration across several services.

7.2 Build risk-based waves

Sequence work according to exposure and changeability, not organisational ownership.

A wave should contain the set of changes needed to alter one material path. For example, “secure privileged access to critical finance services” may combine identity changes, administrator processes, supplier access, logging, legacy application remediation and an exercise.

The wave has one accountable outcome owner even though several teams deliver it.

7.3 Integrate security with change portfolios

Every significant digital, cloud, workplace or supplier programme alters security conditions. Security transformation cannot operate as a parallel portfolio that repairs

decisions later.

Create shared gates at moments when options are still open:

1. Concept: identify material security outcomes and dependencies.
2. Design: resolve identity, data, supplier, recovery and operational ownership.
3. Release: verify control conditions and approved exceptions.
4. Operate: confirm telemetry, capacity, support and response.
5. Renew: reassess when threat, service or supplier conditions change.

Security advisers retain independent judgement, but advice enters the programme before investment hardens the design.

7.4 Fund control operation, not only control purchase

Every business case must include the ongoing work created by the control: alert handling, access administration, exception management, tuning, assurance, training, licence growth and eventual retirement.

A £1 million technology deployment that creates fifteen permanent operational roles is not a £1 million decision. Treating it as one guarantees under-resourced operation.

7.5 Govern exceptions as a portfolio

Individual exceptions can be reasonable while their aggregate becomes intolerable. The programme should group them by cause:

- Legacy incompatibility
- Supplier limitation
- Operational urgency
- Missing ownership
- Insufficient capacity
- Control design failure

Repeated exceptions signal a structural decision. They require investment, redesign, risk acceptance or service retirement.

8. Decision Rights and Roles

Security transformation fails when everyone is responsible and nobody may decide.

The executive sponsor owns the transformation outcomes, prioritisation and cross-organisational trade-offs.

Business service owners accept operational consequences and residual risk within delegated limits. They do not delegate accountability to the security function.

The security leader sets security policy, provides independent advice, operates specialist capabilities and escalates exposure beyond appetite.

Technology and product owners implement and sustain controls within services.

The programme director integrates waves, dependencies, funding, benefits, decisions and transition into operations.

Risk, legal, privacy, audit and commercial specialists challenge and advise according to the nature of the decision.

A decision record should state the service, threat path, options, operational consequence, security advice, residual exposure, accountable decision-maker, conditions and review trigger.

“Security becomes governable when the organisation can see not only which control is missing, but which decision keeps it missing.”

9. Evidence That Matters

The programme needs a small balanced scorecard.

Exposure

- Critical services with verified identity, asset, supplier and recovery maps
- High-risk paths without effective control
- Concentration in identities, suppliers or legacy technology

Control effectiveness

- Critical assets reporting healthy control status
- Privileged access reviewed and anomalous use investigated
- Material vulnerabilities remediated within risk-based times
- Exceptions within expiry and compensating controls verified

Resilience

- Recovery tests completed against agreed service time
- Dependencies that caused test failure
- Backups protected and restoration proven
- Incident exercises completed with decisions and communications tested

Adoption and operation

- Control failure creating user workarounds
- Alert and exception queues within capacity
- Joiner, mover and leaver accuracy
- Supplier access removed when no longer required

The board should ask what exposure changed, what remains, what decision is blocked and whether the operating model can sustain the control.

10. A Twelve-Month Transition

The first ninety days establish the service map, decision rights and two or three risk-based waves. Select critical services where exposure is material and change is possible.

Months four to six deliver the first integrated waves and measure control operation, not installation. Run recovery and incident exercises early; they reveal dependencies faster than documentation reviews.

Months seven to nine embed ownership and funding in service teams. Retire duplicate projects, consolidate exception causes and redirect investment where operating burden is highest.

Months ten to twelve provide independent assurance, renew the service risk view and close waves whose outcomes are demonstrably sustained. The next programme cycle begins from changed exposure, not from a repeated list of controls.

The programme must be willing to stop low-value security activity. A control that consumes substantial capacity while protecting no critical path should not survive merely because it is labelled security.

11. Recommendation

Organisations should establish cybersecurity as a board-sponsored transformation programme that changes the operating model across critical services, rather than continuing with a portfolio of disconnected technical projects.

The recommendation has six commitments:

1. Govern security through critical-service outcomes.
2. Sequence integrated waves around material threat paths.
3. Give business and technology owners explicit accountability.
4. Insert security judgement into existing change before options close.
5. Fund ongoing control operation and govern exceptions collectively.
6. Measure changed exposure, resilience and sustainability.

This model will not eliminate cyber incidents. No honest programme can promise that. It will make the organisation less dependent on emergency mobilisation and more capable of deciding before exposure becomes a crisis.

The lesson of remote work is not simply that the perimeter has gone. It is that technology, operating practice, supplier dependency and human judgement now change together. Security organised as a set of tools will always arrive at only part of that system.

Security organised as a programme can change the system — and then leave it capable of governing itself.